NMC | Media-N
Journal of the New Media Caucus | ISSN: 1942-017X

Art and Anti-Fraud Activism

Andreas Zingerle
University of Art and Design Linz, Austria

Linda Kronman
KairUs Art+Research

Introduction

General tactics of advance fee fraud can be traced back to the early 16th century, where face-to-face persuasion known as the "Spanish prisoner scheme" was widely used to trick victims. Over centuries, the basic scheme has adapted to new modes of communication: letters, telegraph, fax, phone and Internet. A global boom happened in the 80's with growing use of emails, enabling scammers to contact a large number of people fast and very cost efficiently. According to the latest Internet Crime complaint center report, they received over 269,000 Internet crime-related complaints with an adjusted dollar loss of $800,492,073. [1]

There are online communities of so-called "scambaiters" who fight back against online criminals. The act of scambaiting arose as a counterattack to "419 scams." These online vigilante communities investigate scam emails and implement social engineering techniques to document, report, or warn potential victims. Scambaiters are anti-fraud activists who often use similar tactics as scammers, e.g. using social engineering methods to uncover practices of Internet scammers. [2] Scambaiters have their own personal motivations to justify their actions. Their motives can range from community service and status elevation to revenge for being a victim of a similar scam in the past. [3] Through the documentation and sharing of these plots, scambaiters waste the scammers' time, exploit their resources, and raise awareness about online fraud. They organize themselves on forums like thescambaiters.com or 419eater.com. These forums focus on everyday scam types and members follow their own strategies and ethics when in contact with scammers.

So far artworks and academic discussions [4, 5, 6, 7] portray the scambaiting communities as a unified group of people who use xenophobic and humiliating strategies to seek vengeance. Through our research and artworks, we have been able to bring forth a way more diverse scambaiting community and show how various subgroups develop their own practices and strategies to creatively tackle online scams and actively work towards social change in computer mediated online communications. Therefore, our contribution concerns the understanding of the activists' strategies undertaken within different scambaiting communities. These strategies include

- raising awareness about Internet fraud,
- documenting the applied tactics to warn victims,
- jamming the work-flow of scammers and
- reporting vital information to
- diminish and stop Internet fraud.

Over the last years, we followed these communities and created several media art installations that show the activist methods that are used by "Scam Alerters," "Trophy hunters," or "Bank guards." In the following paragraphs, we want to present these communities and take a closer look at their motives and different strategies in form of four of our recent works that tackle issues of digital storytelling and banking loopholes (*Faceless patrons*), data security (*Password: ******* and *Monitoring Harry Brooks*), or focus on the strategies and technologies used in fraud attempts (*Let's talk business*).

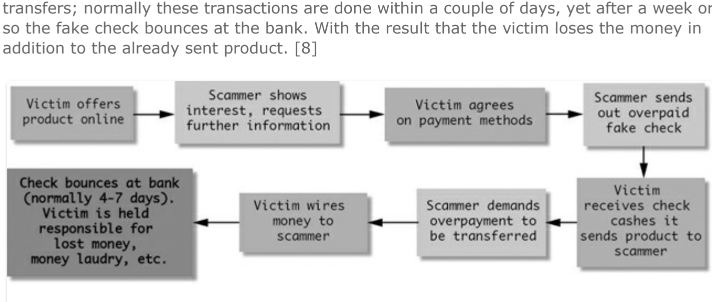
Digital storytelling to report banking loopholes

Some scambaiters specialize in obtaining background information on all kinds of bank related issues like overpaid check validation, phishing sites, money mules, reporting fake banks or closing bank accounts. The so-called "Bank Guards" often target scammers who use bank accounts in their payment procedures, e.g. charity scams. By reporting bank accounts, "Bank Guards" believe that scammers lose money in a legitimate manner or other victims who act as 'money mules' are warned.

Scammers use different tools to divulge personal financial information from their victims: credit card numbers, account username/passwords, social security numbers, etc. Personal documents like passports, birth certificates, and (electronic) signatures can be collected. A scammer can use this information for Identity fraud: starting businesses in the victim's name, open accounts, gaining trust or other benefits in that person's name. Scambaiters try to document and monitor this fraud attempts.

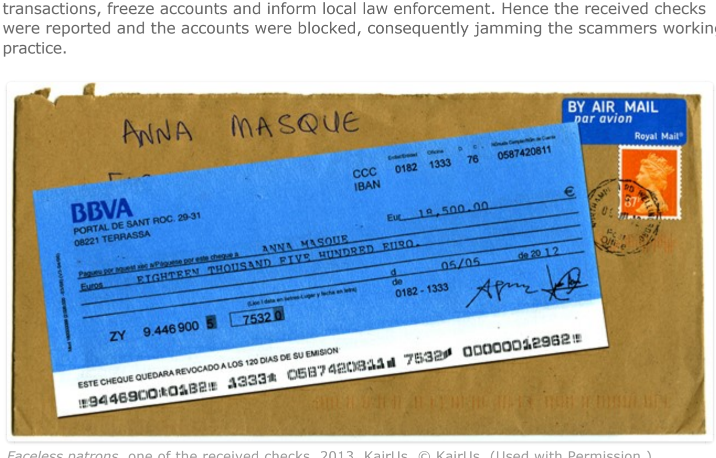
Within the 419Eater.com community, collecting and reporting fake bank accounts can become a game itself, where the challenge is to gather as many accounts as possible within a certain time. Extra points have been given to talented activists who were able to get more than one account information from the same scammer. A special focus was given to fraudsters who run Coca-Cola lottery scams, their bank accounts scored double. To motivate the participants, the winner received a "Premium Membership" of the 419Eater forum to access additional content. The challenge was open for two months and the participating bank guards could report over 160 bank accounts. The sharing of the story plots and tactics with the community results in new efficient methods to counterattack this kind of scammers' practice. By documenting and reporting criminal activities to bank officials, they monitor account transactions, freeze accounts, and inform local law enforcement.

Faceless patrons is an interactive installation that documents stories used by Internet scammers in so called "overpayment check scams." The overpayment check scam is still common although digital payment methods are increasing in popularity. A scammer who shows a certain interest in the offered product contacts a person who offers a product online. The scammer claims that for him it is just possible to pay by check. When the victim agrees to the deal the scammer sends the forged check. The check is issued for far more money than agreed, but the scammer argues that the overpayment is to compensate the shipping costs and for the extra work. The scammer comes then up with a storyline convincing the victim to immediately cash the check, pay the shipping fee and wire the rest of the money to him. The scammers are using a very old loophole connected to the check transfers; normally these transactions are done within a couple of days, yet after a week or so the fake check bounces at the bank. With the result that the victim loses the money in addition to the already sent product. [8]



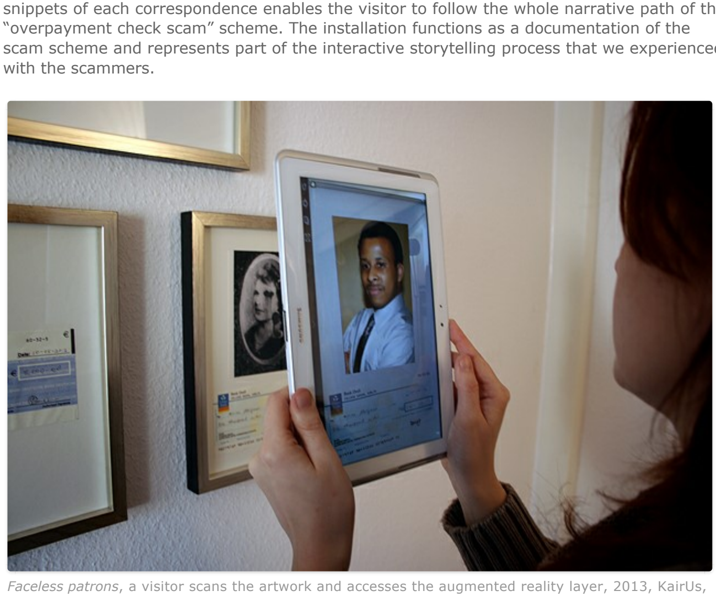
Faceless patrons, the anatomy of the overpayment check scam, 2013, KairUs, © KairUs. (Used with Permission.)

These scammers use scripted stories to reach their victims, yet when correspondence continues, story worlds start to evolve. We created a virtual character to interact with scammers who posed to be art buyers. Each story takes the form of e-mail correspondence where two characters are involved; one art patron created by the scammers and our fictional artist "Anna Masquer." The scammers posed identity is often based on either identity theft or a confusing mix of several existing individuals, giving them the opportunity to remain faceless and anonymous. While we were aware of the fact that we are dealing with scammers, we used a fictional character and narration to investigate how the scammers react to various turns in the plot. Our character Anna Masquer represents an average contemporary artist, and her story is backed up by a virtual identity. [9] We actively engaged with several art scammers, all posed as wealthy art buyers that were immediately interested in the proposed photo series and wanted to pay by check. Anna accepted the check payments and once we received a check we forwarded the ongoing criminal activities to anti-fraud activists who keep good relations with bank officials, who monitor account transactions, freeze accounts and inform local law enforcement. Hence the received checks were reported and the accounts were blocked, consequently jamming the scammers working practice.



Faceless patrons, one of the received checks, 2013, KairUs, © KairUs. (Used with Permission.)

Based on the interaction with the scammers we created an installation setup, that consists of five photo-frames hanging on a wall. Each frame connects to a correspondence with a scammer and holds a photograph and a fake check that was received as an advance payment for Anna Masquers' photos. By using a smart-phone the visitor can scan each photograph via a third party AR-Browser. Each physical photograph is then overlaid with an AR layer containing a video compilation of images. These images are the result of an on-line search in an attempt to confirm or invalidate the authenticity of the scammers' character and his on-line representations. This search result tries to give a face to the faceless scammer, yet fails while the posed art buyer can be anyone or no one of the persons found within the search. Additional to the images, the video contains text-to-speech converted voice-over parts from the email correspondence. Due to the similarity of the scripts that the scammers use snippets of each correspondence enables the visitor to follow the whole narrative path of the "overpayment check scam" scheme. The installation functions as a documentation of the scam scheme and represents part of the interactive storytelling process that we experienced with the scammers.

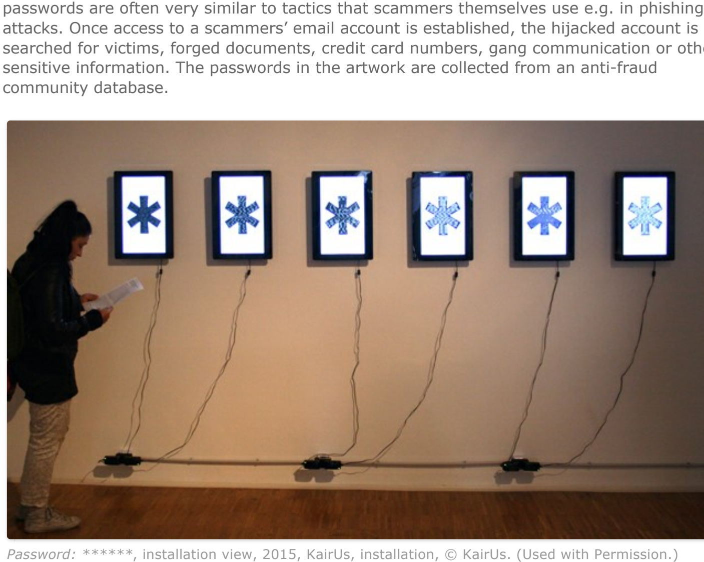


Faceless patrons, a visitor scans the artwork and accesses the augmented reality layer, 2013, KairUs, © KairUs. (Used with Permission.)

Perspectives of data security and privacy

Another subgroup of anti-fraud activists we call "Inbox Divers." These scambaiters are social engineers who log into the scammers email account and warn potential victims or report ongoing criminal activities. This very questionable tactic of browsing through an email inbox gives a very personal insight into the working methods of a scammer. These vigilantes justify the intrusion of privacy with the efficiency of warning victims and disrupting the work of the scammers. Scammers often use email inboxes to store additional information, like other account passwords, documents they use to gain victims trust, email-drafts unveiling their scamming practice or chat conversations with fellow gang members. "Inbox divers" log into the scammers email account to monitor the scammers practices. [10]

The 6-channel video installation *Password:* ****** reveals popular email-passwords used by Internet scammers. The passwords are arranged typographically in six stars, each star containing one of the most used words in the pass-phrases: "good," "love," "money," "mother," "jesus," and "bless." By using storytelling and social engineering techniques as psychological manipulation to gain the trust of the scammer the scambaiters collect and combining apparently non-relevant information, they try to obtain sensitive data to be able to gain access to the scammers' email passwords. The methods to collect usernames and passwords are often very similar to tactics that scammers themselves use e.g. in phishing attacks. Once access to a scammers' email account is established, the hijacked account is searched for victims, forged documents, credit card numbers, gang communication or other sensitive information. The passwords in the artwork are collected from an anti-fraud community database.

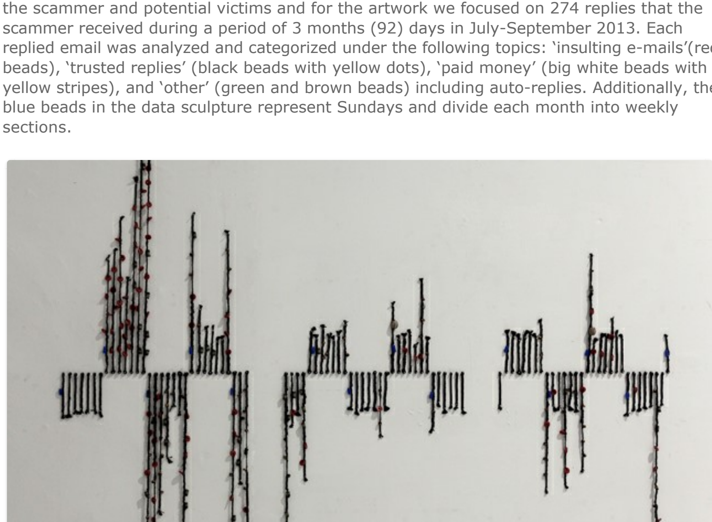


Password: ******, installation view, 2015, KairUs, installation, © KairUs. (Used with Permission.)

To visualize the passwords, we use six video screens, each showing an animated loop of one star. They are hung next to each other and form a six letter password combination. Once visitors approach the artwork they see small typographic password combinations within each star. The subtle animation of changing the contrast of the letters emphasizes capitalized letters, numbers or popular words, demonstrating how little effort we put into creating secure passwords in general.

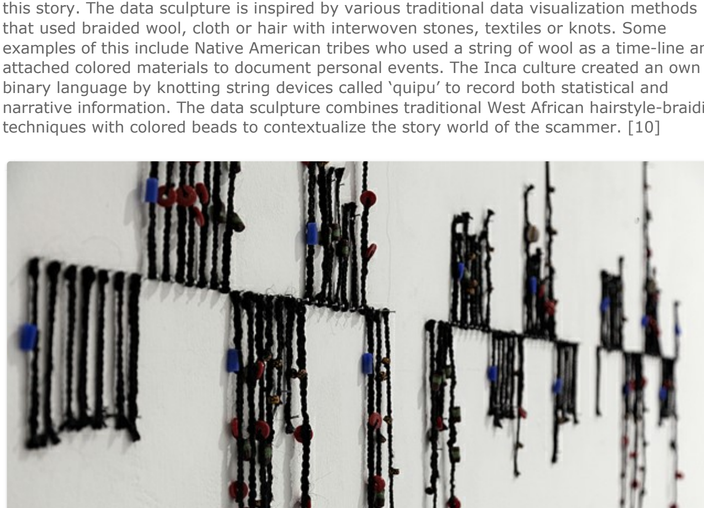
Password: ******, detail view of one star, 2014, KairUs, installation, © KairUs. (Used with Permission.)

Monitoring Harry Brooks is a data sculpture that visualizes 274 email replies that an Internet scammer received during a period of 3 months. By using social engineering techniques, we gained access to the emails of the scammer. [10] We analyzed the correspondence between the scammer and potential victims and for the artwork we focused on 274 replies that the scammer received during a period of 3 months (92) days in July-September 2013. Each replied email was analyzed and categorized under the following topics: 'insulting e-mails'(red beads), 'trusted replies' (black beads with yellow dots), 'paid money' (big white beads with yellow stripes), and 'other' (green and brown beads) including auto-replies. Additionally, the blue beads in the data sculpture represent Sundays and divide each month into weekly sections.



Monitoring Harry Brooks installation, 2015, KairUs, installation, © KairUs. (Used with Permission.)

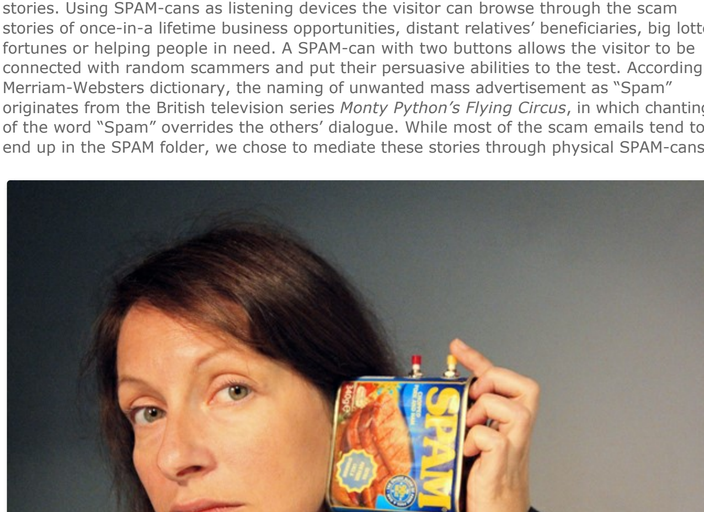
In this inbox the scammer impersonates a U.S. diplomat named Harry Brooks who is based in Benin, West Africa. He seeks assistance to transport a trunk box of $3.7 million US Dollars from Benin to the United States. People who would help him in this confidential mission would receive a share of the secured money. The analyzed e-mail replies are responses to this story. The data sculpture is inspired by various traditional data visualization methods that used braided wool, cloth or hair with interwoven stones, textiles or knots. Some examples of this include Native American tribes who used a string of wool as a time-line and attached colored materials to document personal events. The Inca culture created an own binary language by knotting string devices called 'quipu' to record both statistical and narrative information. The data sculpture combines traditional West African hairstyle-braiding techniques with colored beads to contextualize the story world of the scammer. [10]



Monitoring Harry Brooks, detail view of the installation, 2015, KairUs, installation, © KairUs. (Used with Permission.)

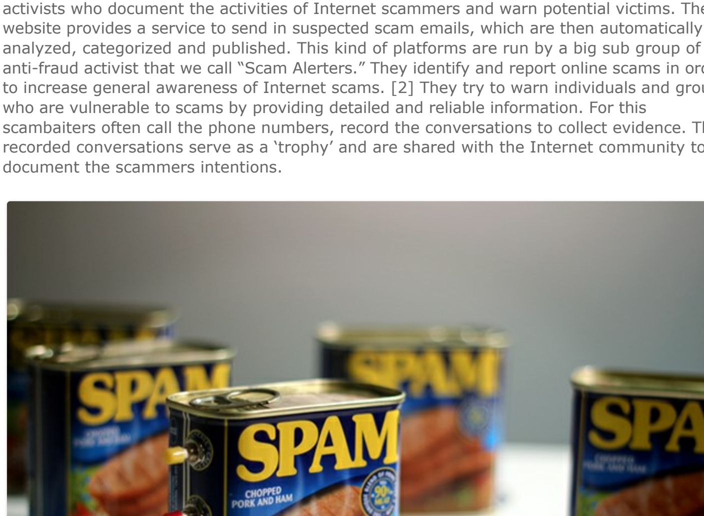
Scams and Technologies

Let's talk business is a multi-channel audio installation that enables the visitor to listen to Internet scammers who try to lure potential victims into advance fee payments. Their phone numbers were extracted from a scam email database, analyzed by country, and categorized by scam scheme. Once we called them, the scammers had the chance to tell their persuasive stories. Using SPAM-cans as listening devices the visitor can browse through the scam stories of once-in-a lifetime business opportunities, distant relatives' beneficiaries, big lottery fortunes or helping people in need. A SPAM-can with two buttons allows the visitor to be connected with random scammers and put their persuasive abilities to the test. According to Merriam-Websters dictionary, the naming of unwanted mass advertisement as "Spam" originates from the British television series *Monty Python's Flying Circus*, in which chanting of the word "Spam" overrides the others' dialogue. While most of the scam emails tend to end up in the SPAM folder, we chose to mediate these stories through physical SPAM-cans.



Let's talk business installation view, 2015, KairUs, installation, © KairUs. (Used with Permission.)

In many of today's fraud schemes phone numbers play an important role. Fraudulent businesses or fake personas can appear more legitimate, and the phone numbers enable a faster, more personal contact to the victims. When scammers setup a fake email address at free web-mail services like Gmail or Outlook, popular VoIP services are included and can be used for free. These tools enable the scammers to hide their identities with fake names and bogus business websites. With the analysis of a sample probe of 374 emails taken from the 'scammed.by' scam email database, we wanted to see which business proposals are commonly used and how believable their proposals sound once we contacted them by phone. In 2010, 'scammed.by' was created under the name "baiterbase," a place for scambaiting activists who document the activities of Internet scammers and warn potential victims. The website provides a service to send in suspected scam emails, which are then automatically analyzed, categorized and published. This kind of platforms are run by a big sub group of anti-fraud activist that we call "Scam Alerters." They identify and report online scams in order to increase general awareness of Internet scams. [2] They try to warn individuals and groups who are vulnerable to scams by providing detailed and reliable information. For this scambaiters often call the phone numbers, record the conversations to collect evidence. The recorded conversations serve as a 'trophy' and are shared with the Internet community to document the scammers intentions.



Let's talk business spam cans, 2015, KairUs, installation, © KairUs. (Used with Permission.)

Closing remarks

We consider our artworks as case studies and through them it was possible to test different scambaiting strategies in order to prove how they can be used as anti-fraud activism. The research has also functioned as a base for discussion, and to raise awareness, as it was presented at several exhibitions and in a series of workshops that were organized in various contexts. A reflective scambaiter with the right intentions can be seen as an anti-fraud activist, who jams the scammers work-flow and alerts potential victims by exposing the scam schemes. This can be done in discussion forums, by collecting databases of dubious mails and phone numbers, reporting fake checks as well as through artworks. By combining art and scambaiting practices we consider it as artivism, a genre where art and activism merge. The research and exploration of various scambaiting methods for the artworks have provided a wider understanding on what the practice of scambaiting is, apart from conventional perceptions, such as the stigmatisation of scambaiters as a xenophobic mob bent on humiliation. These findings clearly contradict to the ongoing publications and help to broaden the definition of scambaiters as diverse communities each with their own strategies.

References

1. IC3, "Annual Report 2014," Accessed May 1, 2016. http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf (accessed May 1, 2016)

2. Andreas Zingerle, and Linda Kronman. "Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies Against Online Advance Fee Fraud." International Conference on Cyberworlds (CW) (IEEE, 2013). Accessed May 1, 2016. doi: 10.1109/CW.2013.49

3. Lauri Tuovinen, et al. "Baits and beatings: vigilante justice in virtual communities." Proceedings of CEPE (2007), 397-405.

4. Dara Byrne, "419 Digilantes and the Frontier of Radical Justice Online." Radical History Review 2013.117 (2013): 70-82. Accessed May 1, 2016. doi:10.1215/01636545-2210464

5. Lisa Nakamura, "'I WILL DO EVERYthing That Am Asked': Scambaiting, Digital Show-Space, and the Racial Violence of Social Media." *Journal of Visual Culture* 13.3 (2014): 257-274. Accessed May 1, 2016. doi: 10.1177/1470412914546845

6. Matthias Krings, "Ein Erzählgenre zwischen interaktiver Fiktion und Hetzjagd im Internet" Marie-Laure, Ryan, *Medien-Erzählen-Gesellschaft: transmediales Erzählen im Zeitalter der Medienkonvergenz*. De Gruyter, 2012, 215–238.

7. John Scannell, "The '419 Scam': An Unacceptable 'Power of the False'?." *PORTAL Journal of Multidisciplinary International Studies* 11.2 (2014). Accessed May 1, 2016. doi: http://dx.doi.org/10.5130/portal.v11i2.3220

8. Autorzy Stabek, Paul Watters and Robert Layton. "The Seven Scam Types: Mapping the terrain of cybercrime." Cybercrime and Trustworthy computing workshop (CTC), 41-51 (2010). Accessed May 1, 2016. doi 10.1109/CTC.2010.14

9. Anna Masquer, "Online portfolio" Accessed May 1, 2016. http://annamasquer.wordpress.com.

10. Andreas Zingerle, "How to obtain passwords of online scammers by using social engineering methods." International Conference on Cyberworlds (CW), (IEEE, 2014). Accessed May 1, 2016. doi: 10.1109/CW.2014.54

Bio:

KairUs is a collective of two artists Linda Kronman (Finland) and Andreas Zingerle (Austria). Their work focuses on human-computer and computer-mediated human-human interaction with a special interest in interactive storytelling. Since 2010 they have worked with the thematic of internet fraud and online scams, constantly shifting focus and therefore approaching the theme from a number of perspectives. Subjects of their research are online scammers, vigilante communities of scambaiters, and their use of storytelling and technology. Besides the artworks the artists also publish research papers related to their projects, and through workshops they contextualize their highly focused research topics from the artworks in broader discourses like data privacy, activism and hacking culture, ethics of vigilante online communities and disruptive art practices. Artworks mentioned in this paper as well as other artworks related to scam, anti-fraud activism and digital interactive storytelling can be found on our website: http://kairus.org/.

scstorytelling can be found on our website: www.kairus.org

PAST EDITIONS